DEFENSIVE INFORMATION OPERATIONS PLANNING TOOL

Final Report

for

Rome Research Site

AFRL/IFGB
525 Brooks Road
Rome, New York 13441-4505

Contract: F30602-99-C-0109

SBIR TOPIC: AF99-141

January 14, 2000

Submitted By:

PREDICTION SYSTEMS, INC.
309 Morris Avenue
Spring Lake, NJ 07762
☎ (908) 449-6800
(908) 449-0897

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (*Leave Blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED

4. TITLE AND SUBTITLE
DEFENSIVE INFORMATION OPERATIONS PLANNING TOOL

5. FUNDING NUMBERS
F 30602-99-C-0109

6. AUTHOR(S)
WILLIAM C. CAVE, ROBERT E. WASSMER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
PREDICTION SYSTEMS, INC
309 MORRIS AVENUE - SUITE G
SPRING LAKE, NJ 07762

8. PERFORMING ORGANIZATION REPORT NUMBER
PSI-99001

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AIRFORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
26 ELECTRONIC PARKWAY
ROME, NY 13441-4514

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
NONE

12a. DISTRIBUTION/AVAILABILITY STATEMENT
UNLIMITED

12b. DISTRIBUTION CODE

13. ABSTRACT (*Maximum 200 words*)

This report describes the SBIR Phase I development and demonstration of a Defensive Information Operations Planning Tool (DIOPT) prototype, which will be used to minimize vulnerabilities and corresponding risks to operations, and interface with existing equipment security monitors and agents running autonomously or cooperatively.

PSI's approach is based on computer technology that affords implementation of the planning tool using a laptop computer. Given operational plans for deploying an Information System (IS), a simulation of the IS can be constructed in the field using graphical icons depicting parameterized models tailored to specific scenarios to be represented. IS planners can construct the simulation by interconnecting icons representing IS nodes and links. Models of threats can be used to assess vulnerabilities of the system to various attacks. Planners can determine how the IS architecture can be improved to reduce vulnerabilities, and predetermine best courses of action to counter an attack.

Once the DIOPT is completely implemented in Phase II, the laptop can be plugged into the actual system to capture real-time data on IS architecture changes, malfunctions or suspected intrusions/attacks. This will cause alarms to summon the planner, to further investigate specified events automatically, and to aid in the rapid determination of the best courses of action to be taken.

14. SUBJECT TERMS
DYNAMIC PLANNING
REAL TIME PLANNING
INFORMATION TECHNOLOGY
INTERACTIVE CONTROL
MODELING & simulation
INFORMATION SYSTEM PLANNING

15. NUMBER OF PAGES
21

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

DEFENSIVE INFORMATION OPERATIONS PLANNING TOOL

Final Report

for

Rome Research Site

AFRL/IFGB
525 Brooks Road
Rome, New York 13441-4505

Contract: F30602-99-C-0109

SBIR TOPIC: AF99-141

January 14, 2000

Submitted By:

PREDICTION SYSTEMS, INC.
309 Morris Avenue
Spring Lake, NJ 07762
☎ (908) 449-6800
(908) 449-0897

1. BACKGROUND

Vulnerability assessment and risk management methodologies for Information System (IS) operations are currently static; they are done periodically, and do not account for the real-time dynamic changes to information system architectures. If vulnerability assessments can be automated to a reasonable degree, using suitably accurate models of the desired information system, then they can be used prior to deployment, as well as on a real-time operational basis.

PSI's SBIR Phase I effort demonstrates an approach to using automated tools to create a Defensive Information Operations Planning Tool (DIOPT) simulation that can be developed and deployed quickly in support of IS operational management, specifically to minimize system vulnerabilities. It is based upon PSI's real-time control and simulation environment that has been used for rapid development of dynamic real-time data and communication systems, including dynamic network management. This environment consists of the General Simulation System (GSS), for discrete event simulation, and the Visual Software Environment (VSE) for building real-time control systems. On top of these tools, PSI has developed a new Run-Time Graphics (RTG) system that allows the analyst to graphically monitor the operation of a live system, in real-time, or a simulation of that system, interactively. This environment is directly applicable to the rapid development of a dynamic real-time IS management tool that will assist in minimizing vulnerabilities and corresponding risks to operations.

2. OPERATIONAL CONCEPT

PSI's approach is based upon computer technology that affords implementation of the planning tool using a laptop computer. New laptops generally provide sufficient speeds of computation, main and auxiliary memory sizes, and graphics to accommodate hardware-in-the-loop functional capabilities required for real-time data acquisition, simulation, and optimization.

Figure 1 is an illustration of the envisioned operation. Given the operational plans for deploying an Information System (IS), a simulation of the IS can be constructed using predeveloped models represented by icons. These models can be parameterized and thus tailored to the specific scenarios to be represented. The IS planner can construct and modify the simulated IS network by interconnecting IS system icons representing predeveloped models of IS nodes and links that the planner understands. Models of threats to the IS system can then be used to assess the vulnerabilities of the system to various types of attacks. This can afford a planner the ability to determine how the IS architecture can be improved to reduce vulnerabilities, particularly to mission critical tasks, and to predetermine best courses of action to counter an attack.

Multi-Tasking Communications Facilities and High-Level Interprocessor Resource Sharing Facilities

Once the IS is operationally deployed, the laptop can be plugged into the actual system to capture real-time data on IS architecture equipment topology, utilization, changes, malfunctions or suspected intrusions/attacks. When the only means of interfacing with the system is external, e.g., using a communications channel, then multiple VSE tasks, each interfacing to a different system via a separate TCP/IP socket will be used. In this case, the VSE task is used to "talk" to the other system using its communications TCP/IP library, and interface to the DIOPT simulation via GSS intertask resources.

As an alternative to the above multi-tasking communications facilities, when the system can accommodate the necessary GSS support module, this interface can easily be accomplished using GSS interprocessor resource sharing facilities. In this case, the *coherency* of data, e.g., as shared between the

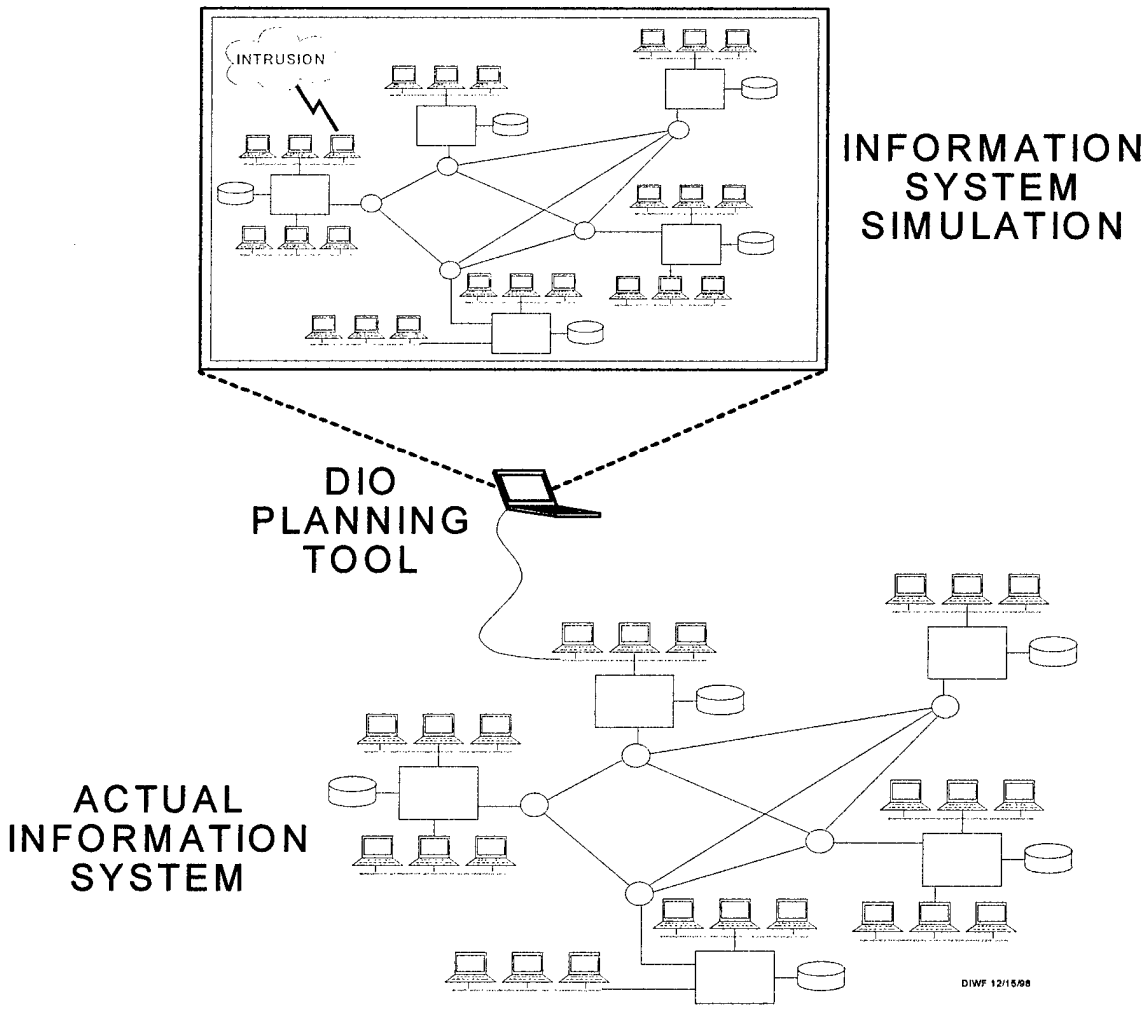

Figure 1. Illustration of the envisioned operational concept.

DIOPT Simulation and the HP OpenView System, the Distributed Agent Information Warfare Framework (DAIWF), or other system, is easily maintained. In either case, alarms will be activated to summon the planner, to further investigate specified events automatically, and to aid in the rapid determination of the best courses of action to be taken.

Creating & Modifying An *IS* Simulation Operationally

The basic premise underlying the planning tool is the ability for an operational planner to easily create a simulation that represents an IS to be deployed, or one that is already deployed. The unique technology developed by PSI provides this facility. Operational planners who are not familiar with techniques of modeling can interact graphically with a simulation *while it is running*. The planner can connect up an IS network using icons and links that are easily understood graphically.

The proposed facility can be used to create a simulation of a new IS, as well as modify an existing IS simulation. In either case, it can be done while the simulation is running. The simulation part of the planning tool is in effect a *virtual* simulation that is used to represent any configuration that can be connected using predefined iconic models. Using PSI's technology, interactively modifying an IS network model, while the simulation is running, is no different from creating a new one.

Having created the simulation of the IS, the tool can be tied into the IS network to detect and decode or otherwise determine any new additions or modifications to the IS or attacks on the IS. This can be accomplished using existing agents in the IS that can send information to the tool regarding status of the IS network. Using iconic models of the IS node and link equipment, the planner can then append or modify nodes and links to bring the IS model up to the actual network.

Assessing Vulnerabilities Of And Improvements To An *IS* Network

To investigate IS vulnerabilities, the planner can pose anticipated types of attacks on the IS at their potential entry points using the simulation (something that is not practical to do on the live system). This implies using previously modeled threats and equipment susceptibilities to create simulated attacks against the IS, and to evaluate their effects on mission critical tasks.

The planner can then categorize and rank the simulated attacks based upon measures of the effects. Attacks can be categorized by type and parameter values, and ranked in accordance with their effects on mission critical tasks.

The planner can pose counters to selected attacks based upon knowledge of the vulnerabilities, potential changes to the IS architecture, and potential shifting of tasks to different parts of the architecture. These counters can be tried and evaluated based upon measures of effects on overall IS performance as well as mission critical tasks.

Using the multiple simulation rerun capability of GSS, tens or hundreds of simulations can be run automatically in very short time periods. These simulations can be run in intelligent sequences to minimize the trials to determine the critical vulnerabilities and the best courses of action. Successful counters can be incorporated into sets of new or modified courses of action against the categorized attacks. This process can be automated using the GSS optimization facilities to determine the best counter measures.

Detecting And Countering Attacks In Real-Time

The system can be designed to detect and decode an event in real time. Events can be detected first by agents in the IS network and passed directly from the IS network to the planning tool, or entered directly by the planner using interactive graphics. Events received directly from the network can cause alarms and actions in the simulation. Using the planning tool, the planner can then proceed to:

- Determine types of attacks, and classify them.
- Determine points of entry.
- Run simulated attacks (of types available based upon current intrusion and point of entry) against the pertinent critical mission tasks and determine the potential effects.
- Rank the potential effects of the simulated attacks based upon measures of these effects.
- Select predetermined courses of action for each type of attack based upon the entry points and criticality of the affected tasks.
- Run the predetermined courses of action to counter simulated attacks and assess the effects.
- Determine new or additional counters where appropriate.

- Incorporate the new or additional counters into the best courses of action and reassess the effects of attacks.

- Update the threat, attack, and counter measure database.

Having completed this process to the best extent possible within allotted time frames, the planner can send the recommended orders to implement the selected courses of action. It is anticipated that most of the above steps can be automated.

3. THE ENVIRONMENT

The combined GSS, VSE, and RTG environment provides a powerful facility for quickly building a tool for visualizing the results of a simulation as it unfolds, or the activities being reported in real-time from a live system. Visually, this is done using hierarchies of icons, lines, and instruments, etc., as illustrated in the prototype DIOPT simulation Figure 2. Each icon can be hierarchical and contain a subhierarchy of various equipment that can be displayed at greater levels of detail, e.g., with the zoomed window view of the information center icon. Without this facility, the graphic display for a very large simulation becomes extremely cluttered, and it is difficult to discern the particular activities of interest at any instant.

When modeling complex systems, if models of computer equipment, routers, radio systems, etc., are designed along physical lines with independent components, then these models are candidates for ease of modification at different protocol layers. Over the past five years, PSI has been involved in reuse of models developed for totally different projects. This has led to careful development of detailed models to insure their ease of reuse in new simulation experiments.

Out of this experience has evolved a new technology - one of creating hierarchical symbolic models that can be interconnected to form higher level models. The actual interconnection is analogous to connecting pieces of equipment together to form a network. Using this technology, the higher level modeler can create network models using icons that get connected graphically, as shown in Figure 2. If the models behind the icons are built correctly, then these interconnections are fed to the models, along with parameter inputs - while the simulation is running. As the equivalent interconnections are recognized by the live equipment, they proceed to operate accordingly.

PSI has implemented high-level interprocessor resource sharing facilities and multi-tasking communications and control facilities, providing for ease of interaction with live equipment monitors such as HP OpenView. PSI has implemented facilities to support the Standard File Interface (SFI) specification that was developed in conjunction with a number of government agencies and contractors. SFI permits users to interchange files easily, and read and write these files using standard library modules available at no cost from a number of sources. SFI provides interfaces to popular database management systems, e.g., FOXPRO, ACCESS, ORACLE, etc., and spreadsheets, data and statistical analysis packages, e.g., EXCEL, LOTUS, SAS, SPSS, etc. PSI will demonstrate this facility as part of this effort.

Interactive instrumentation means that modelers can provide handy instruments for analysts that can take measurements at nodes or between nodes while the simulation is running. This has proved to be a very powerful analysis tool, allowing the analyst to sample various measures of performance at any time during a simulation scenario, and to dynamically change what is being measured based upon the results at that time. The instrumentation facility coupled with the ability to blink, and change the style, thickness,

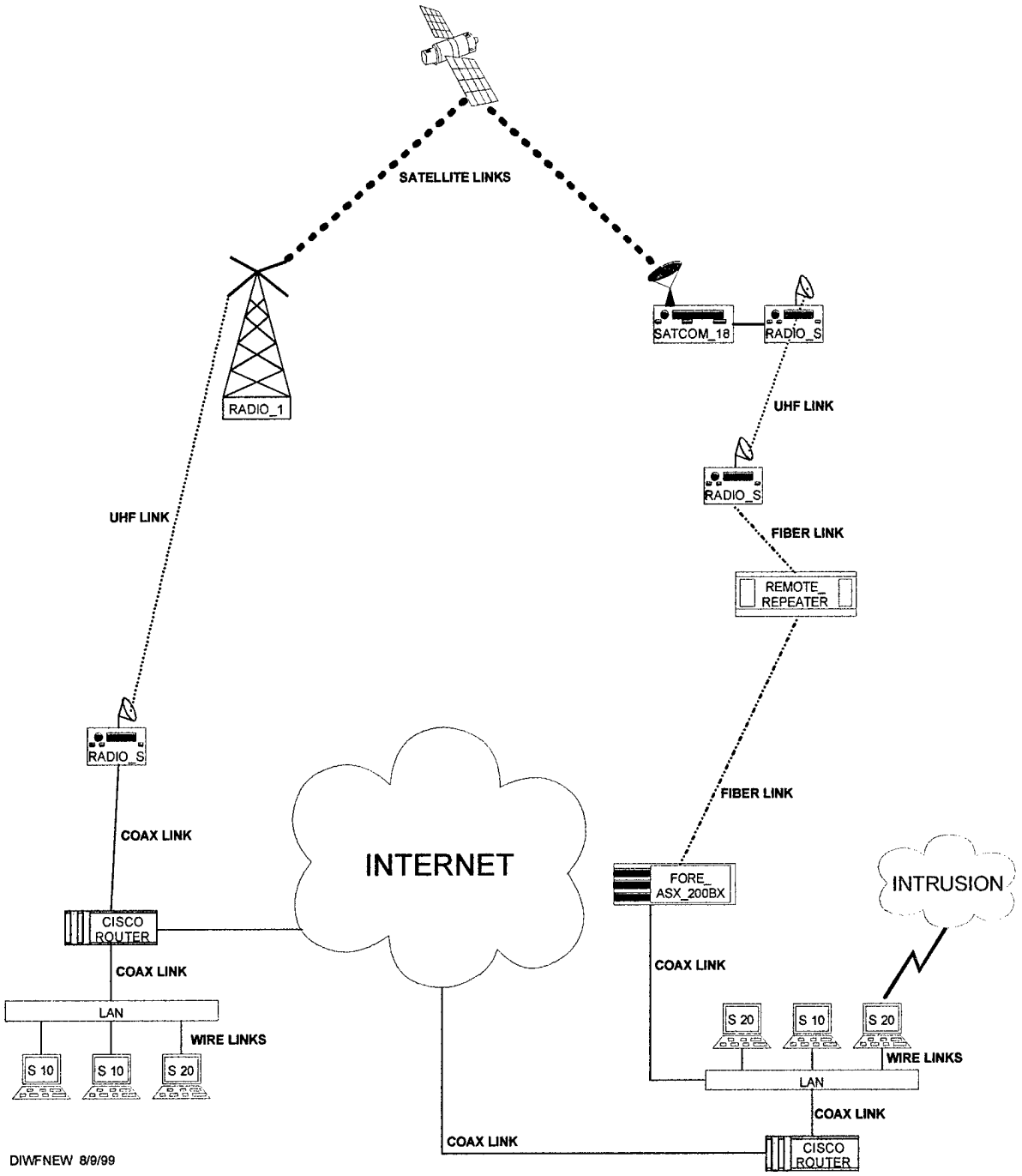

Figure 2. Illustration of the DIOPT simulation with graphic icons depicting physical entities.

and color of network links and nodes, as loading or other properties change during the course of a simulation, provides for excellent visual representations of what is happening in complex systems. This

has afforded modelers the ability to show the dynamics under different stress scenarios so that people with less technical backgrounds obtain a good feeling for the trade-offs of different architectures.

The following sections describe how PSI developed the Phase I simulation aimed at implementing the operational concept of the Defensive Information Operations Planning Tool. Using the existing development environment, and its corresponding tools, we focused on developing a high quality planning tool. Specifically, we focused on designing models that are valid representations of the components of the information system, the system vulnerabilities, and the transient responses resulting from potential attacks on the system. This approach concentrated on building detailed models of equipment operating characteristics, particularly their vulnerabilities, and their responses to different types of attack. Interaction between different pieces of equipment has been modeled to account for spreading malfunctions as a function of time and architecture.

4. PHASE I TECHNICAL OBJECTIVES

The principal objectives for Phase I were (1) the design of a Defensive Information Operations Planning Tool to support Information System (IS) readiness for many years into the future; and (2) the implementation of a prototype to demonstrate the concept and approach. The tool has been designed to support the following primary functions.

- **Creating & Modifying Models of an IS Operationally** - Design hierarchical models of typical IS equipment to demonstrate how they can be interconnected to create a meaningful running simulation during operations.

- **Building *Smart* Network Models** - These models, represented by icons will be the tools used by Higher Level Modelers and Analysts to quickly build "smart" network models in which each element of an information system is already aware of its designated role within the system. The elements of the system are put into action by simply connecting their representative icons into the network

- **Providing Multi-Tasking Communications Facilities** - When the only means of interfacing with another system is external, e.g., using a communications channel, then multiple VSE tasks, each interfacing to a different system via a separate TCP/IP socket will be used as an alternative to interprocessor resource sharing. In this case, the VSE task is used to "talk" to the other system, e.g., HP OpenView, using its communications TCP/IP library, and interface to the DIOPT via GSS intertask resources.

- **Providing Interprocessor Resource Sharing** - Once the IS is operationally deployed, the laptop can be plugged into the actual system to capture real-time data on IS architecture equipment topology, utilization, changes, malfunctions or suspected intrusions/attacks. If the equipment will accommodate the necessary GSS support module, this can easily be accomplished using GSS interprocessor resource sharing facilities, whereby the *coherency* of data, e.g., as shared between the DIOPT Simulation and the Distributed Agent Information Warfare Framework (DAIWF), is easily maintained.

- **Assessing Vulnerabilities of and Minimization Thereof to an IS** - Models of typical IS equipment will contain sufficient detail to demonstrate how they can simulate the results of attacks, and how architectures can be found using optimization to minimize vulnerabilities.

- **Collecting IS Architecture Information in Real-Time** - Interfaces to the IS network will be developed as well as the specification of a generic interface that can be used to communicate with resident Intrusion Detection Systems. The collected information will be used to update the simulation, allowing the existing IS architecture to be analyzed.

- **Detecting and Countering Attacks on an IS in Real-Time** - Interfaces to live equipment will be developed along with representations of agents in the equipment to detect attacks and pass information to the DIO Planning Tool. These agents will also be tasked by the DIO Planning Tool with missions to counter the attacks.

- **On-screen alarms** – The above real-time interfaces can cause alarms to summon the planner to further investigate and aid in the rapid determination of the best courses of action.

PSI has used its real-time control and simulation environment consisting of GSS, VSE and RTG to design and build a prototype of the Defensive Information Operations (DIO) planning tool depicted in Figure 3. This environment provides the framework to quickly build tools to support people in the field who perform real-time analysis and control functions. High quality tools can be built and modified for the field operators by the staff at home, quickly and at minimum cost.

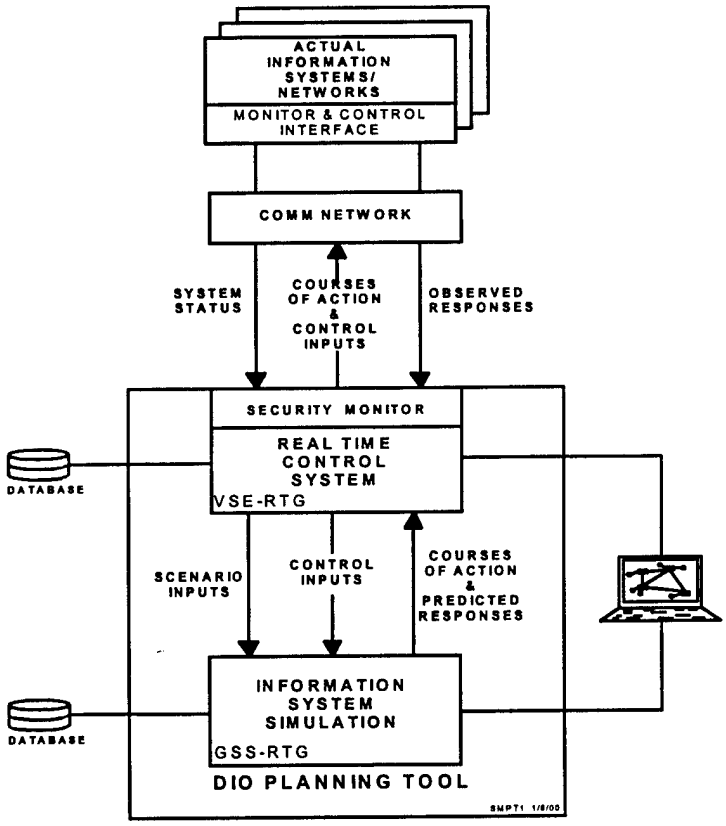

Figure 3. DIO Planning Tool.

Phase I has been used to demonstrate the ease of building, extending, and using the knowledge base that forms the foundation of the DIO planning tool. Specifically, PSI has demonstrated the significant advantages of this new technology by:

- Modeling along physical lines, so that independent models act as the equivalent independent equipments that interact with each other, making decisions based upon their individual rule sets and environments. This makes it easy to understand, modify, and reuse the models.
- Providing engineering drawings of the simulation and the software so that other detailed modelers can understand and change the equipment model architectures provided.
- Providing easy to understand data structures and rule structures so that other modelers can quickly understand and change the databases and rules behind the detailed equipment models.
- Providing easy to use models so that higher level modelers can quickly modify existing models and build new models of IS equipment.
- Providing easy to use implementations of the primary functions of the DIO planning tool so that analysts can think in terms of their own problem and familiar measures of performance, with minimal effort to perform their missions.
- Providing sufficient speed and accuracy of the operations in the implementation so that response times for simulations are sufficiently fast to accomplish the desired result in real time, and so optimization can be used to locate and minimize vulnerabilities.

The completed DIO planning tool must be able to take in and produce various databases, including those that contain parameters for equipment models, deployments, interfaces with other networks, the physical environment, tasks and traffic, the threat environment, and scenario events that can change selected elements of the above. Graphical databases are used to provide tailored graphics, e.g., icons, lines, menus, query templates, and other user interface facilities.

Human interfaces for the DIO planning tool must include interactive graphics, text and numeric prompts, and graphical and textual/numeric hard copy. Models must cover tasks and traffic, information system equipment and networks, the physical environment, threats, and other factors that affect the analysis and planning decisions. Models must provide the ability to insert, modify, or remove selected entities, *while the simulation is running.*

5. PHASE I WORK COMPLETED

In Phase I, PSI develop general models of elements of an information system, including Host Computers, Local Area Networks and Routers connected to the networks, Satellite Systems, and Terrestrial Radio Systems. These models, represented by icons will be the tools used by Higher Level Modelers and Analysts to quickly build "smart" network models in which each element of an information system is already aware of its designated role within the system. The elements of the system are put into action by simply connecting their representative icons into the network. These models are detailed enough that the elements may immediately begin performing their tasks within the network, yet are still flexible enough that they may be modified by a modeler to account for the peculiarities of each individual information system. Modifications can be made by bringing up a parameter template. The critical design criteria necessary to support the functional requirements and the Phase I version of the Defensive Information Operations Planning Tool are now discussed.

Elements of the Phase I DIO Simulation Facility

PSI's approach is based upon computer technology that affords implementation of the planning tool using a laptop computer. New laptops generally provide sufficient speeds of computation, main and auxiliary memory sizes, and graphics to accommodate hardware-in-the-loop functional capabilities required for real-time data acquisition, simulation, and optimization.

Figure 2 is an illustration of the running DIOPT simulation. Given the operational plans for deploying an Information System (IS), a simulation of the IS can be constructed using predeveloped models represented by icons. The IS planner can construct the simulation by interconnecting IS system icons representing predeveloped models of IS nodes and links that the planner understands. Models of threats to the IS system can then be used to assess the vulnerabilities of the system to various types of attacks. This can afford a planner the ability to determine how the IS architecture can be improved to reduce vulnerabilities, particularly to mission critical tasks, and to predetermine best courses of action to counter an attack. Once the IS is operationally deployed, the laptop can be plugged into the actual system to capture real-time data on IS architecture changes, malfunctions or suspected intrusions/attacks. This will cause alarms to summon the planner, to further investigate specified events automatically, and to aid in the rapid determination of the best courses of action to be taken.

The actual network, from individual workstations through LANs, routers, radios and satellites is modeled and represented graphically as the simulation is running. The most important objective of Phase I was to illustrate the ease of building a typical network graphically, using icons representative of the physical entities in the system. A simple traffic generation scheme was also demonstrated, which illustrated messages flowing through the network as it was being built. In Phase II, PSI will extend these models to incorporate detailed internet type and security type protocols that represent the actual system.

The facility can be used to create a simulation of a new IS, as well as modify an existing IS simulation. In either case, it can be done while the simulation is running. The simulation part of the planning tool is in effect a *virtual* simulation that is used to represent any configuration that can be connected using predefined iconic models. Using PSI's technology, interactively modifying an IS network model, while the simulation is running, is no different from creating a new one.

Using iconic models of the IS node and link equipment, the planner can then append or modify nodes and links to bring the IS model up to the actual network. Hierarchical models can be employed whereby a single icon, e.g., a local site is inserted and opened to show internal network hierarchies. These, in turn, are further resolved into their respective elementary models.

Having created the simulation of the IS, the tool can be tied into the IS network to detect and decode any new additions or modifications to the IS or attacks on the IS. PSI has demonstrated this in Phase I with DIOPT simulation running concurrently with an INTRUDER simulation. The INTRUDER simulation attaches to the DIOPT simulation, "invades" the network deployment and connectivity databases, builds an image of the network on its own display, and then "takes out" a router by corrupting the port assignment database of the router. This can be accomplished in Phase II by using existing agents in the IS that can send information to the tool regarding status of the IS network. In Phase II, PSI plans to examine real-time sensor/agent interfaces to the following three systems:

- Distributed Agent Information Warfare Framework (DAIWF)
- Extensible Prototype for Information Command and Control (EPIC2)
- HP OpenView

DIOPT Hierarchical Model Representation in GSS

As presented previously, the General Simulation System (GSS) uses a unique graphical approach to building and storing large quantities of reusable models. GSS includes very high-level modeling languages that enable the user to easily define models of the application to be simulated, and to vary these models for subsequent simulation runs with minimum effort. Figure 4 provides a top-level overview of the DIOPT Simulation. In GSS, the modeler is able to view the entire DIOPT multi-level model hierarchy. GSS supports development of simulations using drawings that contain hierarchical symbolic models. The user creates drawings using a library of symbols as illustrated. These symbols, and the lines that interconnect them, can have different colors and styles that have meaning to the system.

To accomplish this, GSS features a unique separation of the *architectural design* of a system from its *detailed implementation*. This can only occur when the drawings (architecture) provide a one-to-one mapping into the language (code). This one-to-one mapping can only be accomplished when data is separated from instructions. *It is the separation of data from instructions that provides a framework for software visualization.*

As shown in Figure 4, these drawings contain a hierarchy of models constructed from symbols. Developers can pop the covers of higher level icons to see the next layer down, reference Figures 5 through 8. At the lowest level of the hierarchy are *resources*, (data structures) and *processes*, (rules). Users can edit the data and instructions they contain – directly on the drawing. The concepts are quite simple, once one realizes the importance of separating data from instructions, i.e., it is the key to visualization of software. Software is made up of data and instructions. In *GSS*, data is stored in resources, and instructions are stored in processes. These are grouped together to form elementary models. Elementary models can then be grouped with other models to form hierarchical models.

The simulation is currently designed with four top-level models, each with multiple levels of subhierarchy. Most of the work done during the Phase One was directed toward development of a subset of the attached GSS framework for demonstrating proof of concept. Several of the elementary models shown below illustrate the simulation architecture at the GSS process and resource level. In Phase II, all of these model hierarchies will be developed in full detail. The model hierarchy is organized as follows:

- Control Modules - Controls the overall simulation; includes Scenario Control, G2 Control, and Instrumentation submodels. The G2 Control module is used collectively to represent future interfaces to live equipment security monitors such as HP OpenView, DAIWF, EPIC2, etc.

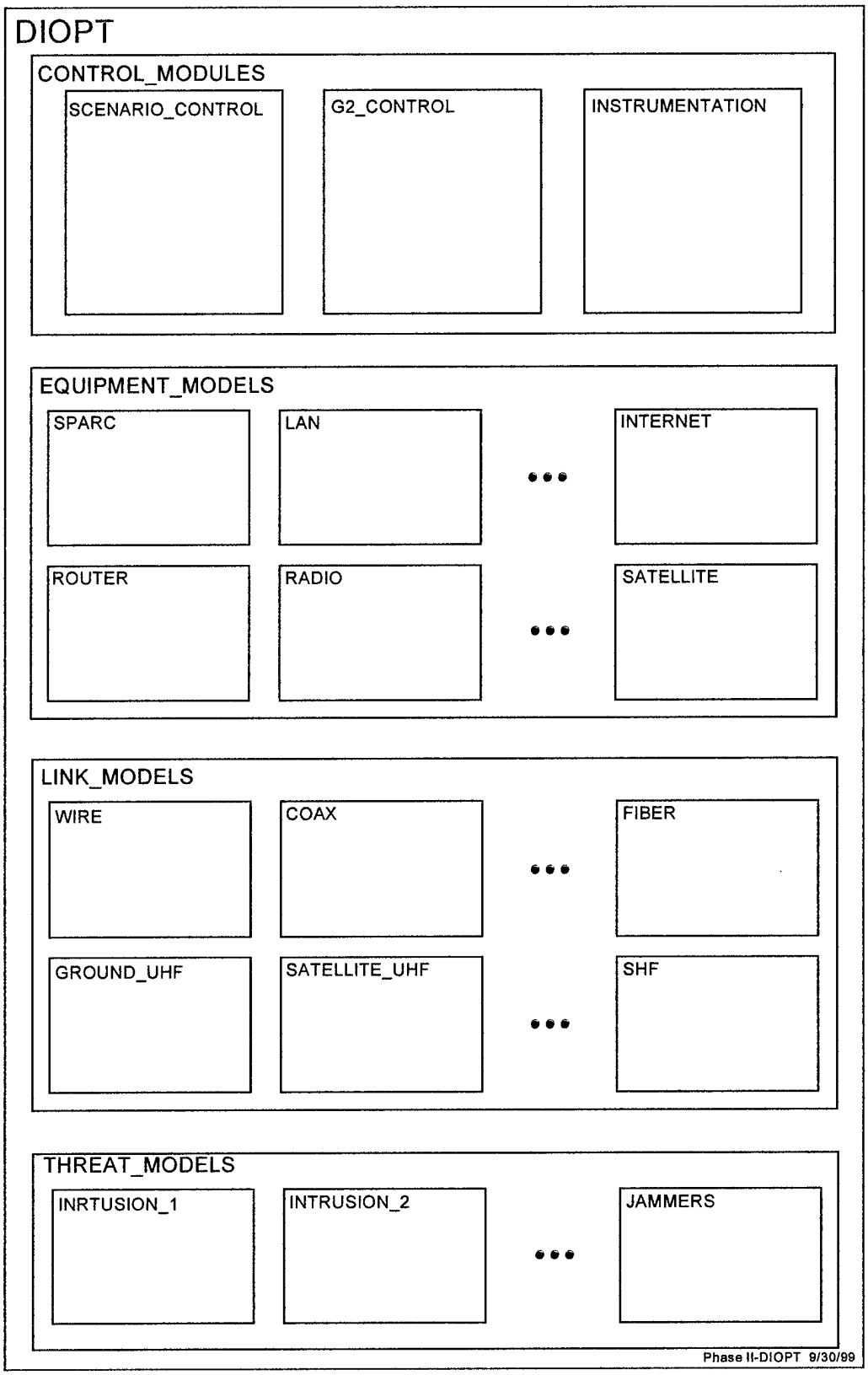

Figure 4. Top Level View of the DIOPT Simulation

- Equipment Models – The equipment used to create communication networks between the data centers that make up the IS, or the subscribers and the data centers; includes Sparc (hosts, terminals), LAN, Router, Radio, Internet, Satellite, and various additional submodels, e.g., firewalls, etc.

- Link Models - Models for all the links comprising the IS network; includes submodels for Wire, Coax, Fiber, Ground UHF, Satellite UHF, and SHF.

- Threats Models - Threat attacks on the IS; includes submodels for Intrusion and Jammers.

The subscriber models and communication and data equipment models are all be instanced and graphically represented with icons. These icons will have specific interconnections that are allowed. For example, a subscriber icon will be allowed to connect to specific icons of communication equipment. Certain communication equipment icons will be allowed to connect to specified data equipment icons. This will allow analysts to connect up a network using the iconic models provided. Networks of equipment will be allowed to be changed, following certain rules, while the simulation is running.

As all of the above models are brought together, the DIOPT Simulation, running in the General Simulation System and GSS Run-Time Graphics system environment is illustrated in Figure 2. Multiple equipment types are linked in this example network, along with intruders and instruments measuring various measures of performance. Having discussed a typical run-time simulation graphic view and the top-level model structure in Figures 2 and 4, respectively, subordinate model layers are presented in the following sections.

5.1. CONTROL MODULES

Scenario Control Module

The scenario control model is at the top level of the DIOPT model hierarchy. The scenario control model is used to determine the quantities of subscribers, types of equipment and their interconnections, as well as individual equipment characteristics, reference Figure 5.

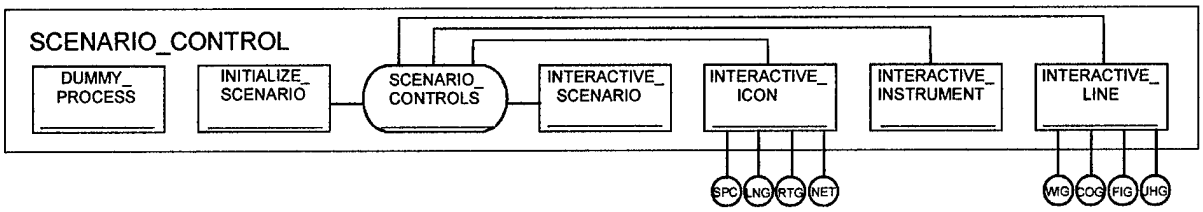

Figure 5. Scenario Control Model

Scenario control can be employed using several different methods depending on the specific objective:

- Interactive Graphics– The DIOPT simulation can be started using a "blank screen," whereby the modeler can interact graphically with the simulation and quickly configure a laydown by inserting predefined hierarchical icons from a menu of available equipment profiles. This can be followed by inserting lines between the equipment icons, thus defining the network hierarchy. This process can be continued through the inclusion of threat elements, etc., to the point where the entire scenario has been defined interactively.

- Scripted Scenarios – The GSS environment supports importing scripted scenario files as external data files, where the user has total control over the record format. These files could have been built as output from prior GSS simulations, output from other simulation environments, direct sensor output, or using various database management systems. These files are read during initialization and corresponding model parameters are set accordingly.

- Live Equipment Interfaces -The G2 Control Module provides a direct interface between the G2 submodels of the GSS DIOPT Simulation Equipment models, and the OpenView, EPIC2 and DAIWF systems. GSS and the three G2 systems all run as autonomous systems, with GSS sending and receiving updates to each of them.

- Standard File Interface (SFI) Files - Most simulations require large time-sequenced data files for both scenario input and collection of output. Special routines have to be written for each new data file, with each file typically formatted uniquely. Also, one would like to have standard interfaces to available database management packages as well as spread sheets. The SFI approach simplifies reading and writing large sequential data files, and has evolved in consideration of all of the above issues. These include creation of the raw data files, editing of input data, and providing for standard file input to, and output from, a simulation so that users do not have to build data input and output modules for each file. SFI also provides for standard reporting facilities that handle header information and page counting.

Of course, it is also probable that some combination of the above methods will be used for maximum efficiency. For example, a standard test scenario could be read from either an external or SFI file, and then used to update the graphic scene automatically. One could then refine the scenario interactively depending on the unique requirements of a particular simulation. Finally, the results of this simulation could be output to an SFI file, and used as an archive of results or as input in support of multiple simulation reruns from the same starting point, forward.

Instrument Module

The instrumentation of the models so that data can be collected to assess the effectiveness of an attack and its potential counters, is show in Figure 6.

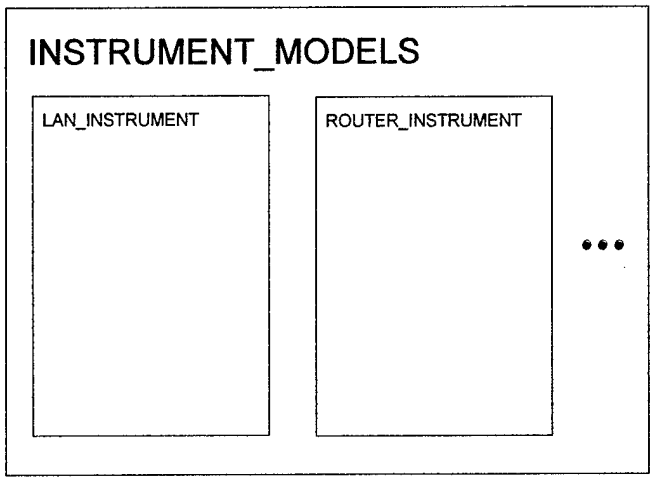

Figure 6. Instrument Models

Measures of the effects of attacks will be shown on the graphics workstation while the simulation is running. The icon shapes will indicate the type of equipment being deployed. The style and thickness of the links will indicate the type of link. The colors of the nodes and links will indicate their state of utilization. The node and link style and color will also be used to identify potential vulnerabilities. Graphical instruments will be used to indicate various scenario performance measures that will be continuously updated as the simulation is running, e.g., the percent of mission critical task requirements currently being met.

5.2. EQUIPMENT MODELS

The data system equipment models characterize the physical and functional attributes of an information system. They will specify the equipment in an IS node, the connectivity, and operating parameters such as the maximum supported capacities and processing delays. Nodes can also be deployed interactively, with affiliation databases updated automatically. This node affiliation information is stored in the RTG ICON database. When new graphical icons are deployed, connected, or removed interactively, this database is updated automatically, and a corresponding message is sent back to the simulation containing the update information.

The architecture of the IS node equipment models, reference Figure 7, provides for increased resolution for representing processing times, data storage capacities, access times and transfer rates, routing and switching transfer rates, and specific response times. Equipment models include classification of susceptibilities and resulting effects corresponding to types of attacks. Node models can be reinitialized for replay purposes. Node characteristics can be taken from a scenario database or input by the user.

The top-level view of the DIOPT Simulation illustrated in Figure 4, shows the Equipment Models opened to the submodel level, where the SPARC, LAN, ROUTER, RADIO, INTERNET and SATELLITE, etc., models are represented. Figure 7 illustrates the *push-down* of two of these submodels, SPARC and ROUTER, through several additional layers, down to the GSS resource and process level. The SPARC submodel is discussed here as a typical example of a model hierarchy. In Phase II, all of the equipment models will be represented in detail.

Sparc Equipment Model

Sparc Administration

The SPARC ADMIMISTRATION model processes events arriving either graphically or through the various simulation interfaces. Using an insert equipment activity as an example, the administration model will create a device address for the inserted SPARC instance, initialize its port address database for eligibility into the network, and initialize other equipment characteristics specific to the SPARC.

Sparc Processes

The SPARC PROCESSES model will interface with the link model to update its device address as its connections up and down the network hierarchy are modified. It will provide its own device address as needed to support other element address updates, and will maintain port addresses for the other network elements to which it is connected. It will also log incoming messages and initiate new messages based on interaction with the subscriber model.

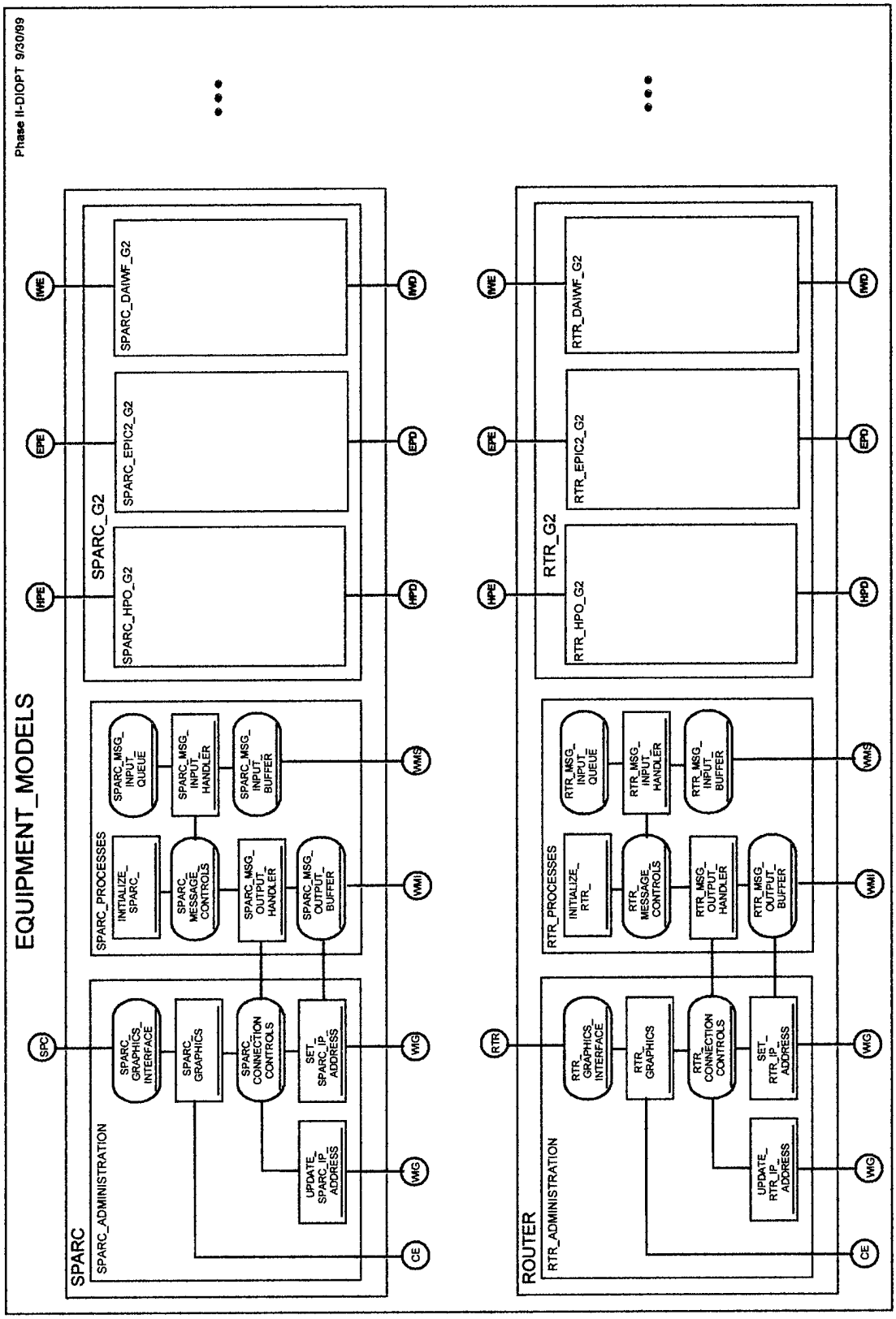

Figure 7. EQUIPMENT_MODELS

Sparc G2

The SPARC G2 model will process real-time inputs/updates relating to topology, security and activity state information maintained in the OpenView, EPIC2 and DAIWF databases. In Phase II, the G2 CONTROL MODULE will interface with these systems directly, and provide real-time inputs/updates to these systems based on the state of the simulation, and receive updates from these systems where pertinent.

5.3 LINK MODELS

The LINK MODELS submodel shown in Figure 8, is used to create communication links between the data centers that make up the IS, or the subscribers and the data centers. An input link database will contain information on node connectivity. Links can also be deployed interactively, with affiliation databases updated automatically. As indicated above, this node and link affiliation information is stored in the RTG ICON database. When new graphical icons are deployed, connected, or removed interactively, this database is updated automatically, and a corresponding message is sent back to the simulation containing the update information.

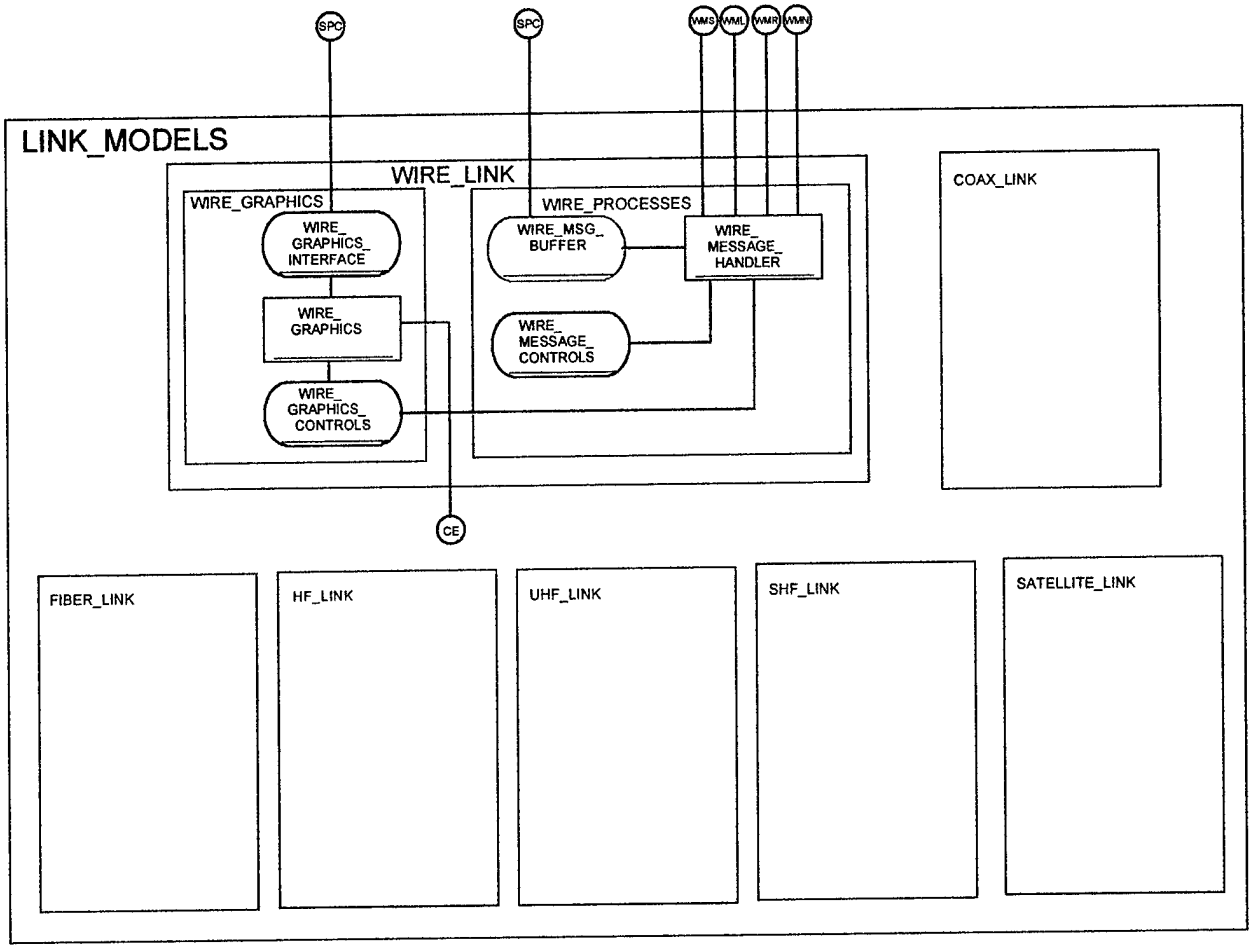

Figure 8. Link Models

Each link will have associated with it the identification of the node on each end of the link, throughput, capacity, and propagation delay. Links can also be deployed interactively, with databases being updated automatically. Several link models will be supported such as wire links, optical fiber links,

and point-to-point radio links. Point-to-Point radio links will have signal-to-noise parameters that will be used to determine link capacity and delay. These can be computed dynamically.

The architecture of the communication network equipment models will provide for increased resolution for representing radio characteristics, capacity throughput and response times. Link models will contain susceptibility characteristics corresponding to specific types of attack.

The link databases will contain information about the physical and functional attributes of a link in a deployment. It will specify the connectivity, and operating parameters such as the maximum supported capacities and processing delays. This link affiliation information is stored in the RTG ICON database. When new graphical icons are deployed, connected, or removed interactively, this database is updated automatically, and a corresponding message is sent back to the simulation containing the update information. To support the analyses of potential deployments, the communication network equipment models will contain routing algorithms to find paths satisfying the data transfer requirements. Models will support the identification of alternate paths if more than 1 path exists. This will be accomplished using the hierarchical icon database, as well as the node and link element databases.

The architecture of the routing protocol models will provide for new or modified protocols. Protocol parameters can be taken from a scenario database or input by the user.

5.4 THREAT MODELS

Intrusion Models

In addition to the intrusion events processed through the G2 interface, the DIOPT simulation will contain direct support for intrusion input either through scripted scenarios or interactively via run-time graphics. It will also be possible to perform optimization simulations designed to maximize the impact of intruders on the current state of the network. This type of input could easily be stored during the optimization simulation and then input to the analysis simulation using the Standard File Interface (SFI).

5.5 INTERACTIVE GRAPHICAL INTERFACES

The simulation has made extensive use of the Run-Time Graphics (RTG) features to provide comprehensive user interaction capabilities with a user-friendly interface. Graphical elements include the following:

- Hierarchical icons to avoid screen clutter when viewing large networks;
- Instruments to indicate the values of predefined measures of merit;
- Links with an assortment of colors, styles, and thicknesses to indicate utilization, connectivity, etc.;
- Menus and templates to provide specific decisions and values for users to select.
- Legends to provide predetermined information content.

RTG provides the ability to pick and select entities, and to cause actions to be taken on the selected entities. Actions can be taken by the simulation or by the user interactively. The set of allowed interactive user actions can be predetermined.

Graphical interactions can be recorded in output files that can be used as input files to reproduce the order of deployment updates. Alternatively, the input files can be converted from other file formats or edited by hand to script the simulation events. Deployment output and input files will have the same format for easily reusing output files as input files. Scenarios can be run entirely from input files if desired.

Background overlays can be provided that show terrain contour lines. These contour lines will be drawn from the same NIMA database containing the terrain elevations used for calculating radio wave propagation path loss. This provides direct correlation between connectivity and position on terrain as seen by the user. Background overlays can also contain foliage, waterways, highways, towns, and gridlines.

Measures of the effects of attacks will be shown on the graphics workstation while the simulation is running. The icon shapes will indicate the type of equipment being deployed. The style and thickness of the links will indicate the type of link. The colors of the nodes and links will indicate their state of utilization. The node and link style and color will also be used to identify potential vulnerabilities. Graphical instruments will be used to indicate various scenario performance measures that will be continuously updated as the simulation is running, e.g., the percent of mission critical task requirements currently being met.

6. SUMMARY OF PHASE ONE RESULTS

During the December reporting period, PSI completed final Phase One upgrades to the Defensive Information Operations Planning Tool demonstration. Satellites and radios have been added to the network elements which can be deployed on the top two levels of the network hierarchy. These elements can be deployed as part of an initial network laydown, and then various user interaction can follow. After the initial network is built, the modeler inserts network elements, connects them, and observes network traffic, device addresses, and port assignments. As the simulation continues, instrumentation can be added, and the results of intrusion can be observed as links are added and deleted, and message traffic is rerouted accordingly. The initial network elements are deployed and connected as defined in Standard File Interface (SFI) input files.

An intruder model has also been added to provide an initial demonstration capability, and establish a framework for the Phase II effort. This model now runs in a separate INTRUDER simulation, which can either be on the same physical computer as the DIOPT simulation, or on a separate computer networked to the DIOPT simulation. These facilities will be expanded in Phase II to take inputs directly from on-line sources to create new scenarios as well as update existing scenarios. These facilities will include direct connections to operations monitors, e.g., HP Open View. This will provide for automatic capture of the identity of equipment in the network, their topological connectivity, and the levels of traffic.

As the INTRUDER simulation begins to execute, it attaches to the DIOPT simulation, "invades" the network deployment and connectivity databases, and builds an image of the network on its own display. The INTRUDER simulation then allows the insertion of an intruder device onto the simulation graphic scene. As this intruder is connected to any LAN, the "intrusion activity" will proceed to migrate from the INTRUDER to DIOPT simulation, and then traverse the LAN-RTR link in the DIOPT simulation, if one exists, and "take out" the RTR by corrupting its port connection database. At this point, all traffic being routed through the corrupted RTR is lost, and future traffic is prevented. The simulation will support the rerouting of traffic around the corrupted RTR, if alternate routes exist. Instruments can be used to illustrate the post-intrusion traffic patterns.

With the completion of this function, PSI believes it has met all of the objectives of Phase One, and has exceeded them in several areas, reference Section 6.2, below. Furthermore, the multi-computer demonstration of the DIOPT and INTRUDER simulations running concurrently proves the technical feasibility of the proposed approach.

As we proceed into Phase Two, the Defensive Information Operations Planning Tool will become a full-scale real-time information systems management planning tool that will assist in minimizing vulnerabilities and corresponding risks to operations. This tool will interface with existing security monitors and agents, running autonomously or cooperatively. Sections 6.1 and 6.2, below, provide a summary of the Phase One version of the DIOPT demonstration, and a summary of additional functional objectives realized.

6.1 DEFENSIVE INFORMATION OPERATIONS PLANNING TOOL DEMONSTRATION

A typical example of the DIOPT and INTRUDER simulation demonstration, which initializes a network automatically, and then allows user interaction in both simulations, can be run by following the steps:

- Enter GSS and run the DIOPT simulation.
- Observe the automatic deployment and connectivity of the initial network.
- In a separate user directory, enter GSS and run the INTRUDER simulation. Observe the capture of the current network running in the DIOPT simulation.
- Click *icon* and deploy optional additional elements in a top-down hierarchy using the NET, RTR, LAN, and SPARC symbols with a single NET at the top, an increasing number of RTRs and LANs in the middle, and multiple SPARC hosts at the bottom.
- Upon completion of the deployment, observe the device IP addresses that are assigned based on position in the hierarchy, and instance of the device.
- Connect these devices by clicking *line*, and inserting lines between appropriate pins on the devices. Most of the lines should traverse down through the hierarchy, but several RTR-RTR and LAN-LAN lines will enhance the demonstration. Devices can be connected in any sequence.
- Upon completion of the connections, observe the updated device IP addresses based on the path up the hierarchy. At any time, the port assignments for a particular device can be observed by picking the device (confirmed by a green outline), and then clicking *ports*. A legend will appear indicating the device type and address, followed by the port numbers and their addresses. The legend can be dropped from the scene by clicking *legend*.
- Messages will automatically be sent and received through successive pairs of SPARC host instances where a path exists at the time of connection of the even numbered instance. For example, as SPARC instance 2 is connected to the network, a message will be sent to instance 1 if a path from 2 to 1 exists (similar dialogues will occur between instances 6 and 5, 10 and 9, etc.). If the path is established after connection of the even numbered instance, the dialogue will not be initiated. Messages will continue to be

sent/received, as long as there is a path between pairs, for the duration of the simulation. The path the message takes will be illustrated with green and red "tracer" lines. If a link is "taken out", messages with no alternative path will be dropped.

- Instruments can be used to track received messages on any device in the network. Simply click *inst* and insert a line between the instrument and the device.

- Routing is dynamic and messages will take the "lowest" available path through the network, e.g., if two SPARCs are connected to the same LAN and are also connected to each other, the message will be sent directly (avoiding the LAN).

- Messages having multiple paths to their destination can be observed to take a higher route after deletion of a lower route. Likewise if a lower route is inserted, messages will reroute accordingly. Multiple instruments are useful to track the load on the various devices as links are inserted and deleted.

- Multiple intruder devices can be deployed on the INTRUDER simulation graphic scene. The "intrusion activity" will then proceed to migrate from the INTRUDER to DIOPT simulation. As the intrusion arrives at the DIOPT simulation, if the affected LAN is connected to a RTR, the intrusion will proceed to traverse the LAN-RTR link, and corrupt the RTR port connection database. At this point, all traffic being routed through the corrupted RTR is lost, and future traffic is prevented. The simulation will support the rerouting of traffic around the corrupted RTR, if alternate routes exist. Instruments can be used to illustrate the post-intrusion traffic patterns.

6.2 ADDITIONAL FUNCTIONAL OBJECTIVES REALIZED IN PHASE ONE

In addition to the specific technical objectives relating to the initial DIOPT model base and demonstration simulation, we believe the following broad functional objectives have been realized:

- **Visual Interactive Modeling** - Create new models, visually, using interactive graphics, by interconnecting icons representing previously developed lower level models to form more complex model hierarchies. Change model parameters via menus and tables for prompted input values. Do this *while the simulation is running.*

- **High Level Security Monitor Interface** - High level security monitors as well as individual equipment agents running autonomously can provide information on intrusions detected, missions performed to counter attacks, and results observed. This information can be used by the proposed tool to analyze the overall threat and attack situation in real-time, and determine architectural level counters to support overall mission tasks.

- **Closed-Loop Experimentation** - Interact with live systems as well as the simulation, making changes and watching the results in real-time, using convenient visual representations of instrumentation to depict the responses, dynamically.

- **Scenario Development and Analysis** - Interface with the Standard File Interface (SFI) and popular database management systems, e.g., FOXPRO, ACCESS, ORACLE, etc. for creating and maintaining large scenario databases. Interface with popular spreadsheet and statistical

analysis packages, e.g., EXCEL, LOTUS, SAS, SPSS, etc., for performing data and statistical analysis tasks.

- **Virtual Model Hierarchies** - Create hierarchies of models by attaching models into subhierarchies and subhierarchies into more complex hierarchies. Be able to change the hierarchical structures to test the results of each. Do all of this *while the simulation is running* as well as in an off-line icon library management drawing board facility.